

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

-----X  
ALBERTO MATTA,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.  
-----X

**ORELIA E. MERCHANT, United States District Judge:**

Petitioner Alberto Matta (“Matta” or “Petitioner”), an Italian citizen, was detained and questioned by federal agents (“the Government”) upon his entry into John F. Kennedy International Airport (“JFK”) in October of 2023. The Government then seized Matta’s cellphone and laptop which were then subjected to an off-site manual forensic search. While his physical devices were later returned, Matta filed the instant motion pursuant to Fed. R. Crim. P. 41(g), styled as a “Motion for Return of Property” (“Motion” or “Mot.”), ECF 1. In his Motion, Petitioner seeks the following relief: (1) the return of all copies of contents/data/information taken by the Government from his electronic devices and (2) to have the Government identify all searches or reviews conducted on his devices. *See* Memorandum of Law for Motion for Return of Property (“Pet. Memo”), ECF 1-8.

Upon consideration of the full record,<sup>1</sup> and for the reasons outlined below, Petitioner’s Motion is GRANTED insofar as the Government must delete all copies of any data or contents taken from Matta’s cellphone and laptop, but DENIED to the extent that Petitioner seeks to compel a list identifying the Government searches conducted on his devices.

---

<sup>1</sup> The Court has considered the parties’ briefs, declarations, representations, statements made at oral argument held on February 6, 2024, and supplemental briefs and declarations filed thereafter. Unless otherwise noted, the facts set forth herein are undisputed.

## FACTUAL BACKGROUND<sup>2</sup>

### A. The Parties

Alberto Matta, an Italian citizen, is the founder, chairman, and majority shareholder of a Luxembourg-based real estate and private equity firm, Optimum Asset Management (“Optimum”). Alberto Matta Declaration (“Matta Decl.”), ECF 1-6 at 1. Optimum is a European “real estate private equity alternative investment manager that invests in projects in United States and Europe on behalf of primary institutional investors.” Declaration of Andrea Suriano in Support of Petitioner’s Motion for Return of Property (“Suriano Decl.”)<sup>3</sup>, ECF 9-1 ¶ 3. “Optimum has offices in the United States and in Europe and manages, *inter alia*, Optimum Evolution Fund SIF (“Optimum Fund”), an umbrella investment fund based in Luxembourg.” *Id.* ¶¶ 3-4. In addition, Matta is also the founder of Futura Funds (“Futura”), “a European regulated private equity firm that manages Futura Funds SICAV Plc (“SICAV”), an umbrella investment fund based in Malta.” *Id.*

Since 2012, Matta has routinely traveled into the United States and has since expanded his business interests here. Redacted Declaration of Special Agent [REDACTED] (“SA [REDACTED]” dated February 16, 2024, (“Feb. Decl. R.”),<sup>4</sup> ECF 16 ¶ 9. In 2014, the United States granted Matta an investor visa predicated on Optimum/Matta’s investment of capital in the United States. Since that time, Matta’s United States-based real estate investment firm, Optimum Development USA LLC, has actively invested in residential and commercial properties in New York, Florida,

---

<sup>2</sup> Several relevant facts are alleged in declarations filed *ex parte*, under seal and unavailable to the public. Those facts shall be redacted on the public docket.

<sup>3</sup> Andrea Suriano is the General Counsel of Matta’s firm Optimum Asset Management S.A. and Head of Legal for Futura, an umbrella investment fund related to the Optimum Fund. Suriano Decl. at 1-2.

<sup>4</sup> SA [REDACTED] is a Homeland Security Investigations enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code. SA [REDACTED] redacted declaration was submitted by the Government as part of *ex parte* sealed communications the Government had with the Court regarding the Government’s purported reasonable suspicion.

and California, including the sale of the largest hotel development on Ocean Drive in Miami, Florida, in 2021. *Id.* ¶¶ 9-10. These acquisitions and sales have been through more than a dozen special purpose vehicles (“SPVs”) incorporated in Delaware and Florida, including an SPV set up as recently as 2020. *Id.*

While not a party to this matter, the Vatican Bank, formerly known as the Institute of Religious Works (“IOR”), is another key figure in this dispute. The Vatican Bank is a Vatican City-based financial institution run by the leadership of the Catholic Church. Suriano asserts that the Vatican Bank is a “defaulting investor in one of [Optimum’s] funds” which resulted in years of contentious litigation against Matta, Optimum, the Optimum Fund, Futura, and the SIVAC (collectively the “Optimum Parties”) where “the Vatican Bank has suffered repeated losses in court proceedings in various jurisdictions in Europe.” Suriano Decl. ¶¶ 2,5,6.

#### **B. Government Investigation of Matta Prior to October 7, 2023**

According to the Government, Matta is the subject of at least two investigations by the [REDACTED]. Matta is also a subject in one domestic U.S.-initiated investigation. SA [REDACTED] is the liaison between the United States Department of Homeland Security Investigation (“HSI”) [REDACTED]. Declaration of SA [REDACTED] dated February 16, 2024 (“[REDACTED] Feb. Decl.”), ECF 13-1.

##### **1. Investigation 1: Gendarmerie’s Investigation into General Fraud Perpetrated against the IOR**

Sometime in August 2022, [REDACTED] [REDACTED]  
[REDACTED]  
[REDACTED] which the Court terms “Investigation 1.” [REDACTED] Feb. Decl. ¶ 4. HSI Rome agreed to aid [REDACTED] and SA [REDACTED] asserts that HSI Rome also initiated its

own investigation to identify violations of U.S. laws concerning a “fraud scheme.” *Id.* The record before the Court does not provide further information as to the purported fraud scheme or its timeframe. Importantly, in the submissions before the Court, neither Matta nor his affiliated funds are alleged to be implicated in Investigation 1.

## **2. Investigation 2: [REDACTED] Investigation into Matta in Connection with the Sale of BSE Building**

In September and October of 2023, [REDACTED]

[REDACTED] Feb. Decl. ¶ 5. The Court terms this as “Investigation 2.” Investigation 2 involves activity that took place sometime in 2012-2013 when the Vatican Bank agreed to invest approximately 200 million euros into the Kappa Fund (“Kappa”), a sub-fund of the SICAV, through an Optimum sub investment fund—Ad Maiora—which is managed by Matta and Optimum. [REDACTED] Feb. Decl. ¶ 6; *see also* Suriano Decl. ¶ 8.

In early 2013, one of the initial investments made with the IOR funds through Ad Maiora was the purchase of the old Bulgarian Stock Exchange building (“BSE Building”), a prestigious historical building in the heart of Budapest, for approximately 32 million euros by acquiring a majority of the shares of its then-owner entity. [REDACTED] Feb. Decl. ¶ 7. However, in November 2013, the Vatican Financial Intelligence Authority discovered that the BSE Building had been bought “several months prior to the sale” by a Matta-owned entity for 12 million euros less than it had been sold to Ad Maiora. *Id.* SA [REDACTED] declares that Matta “did not formally disclose” this prior sale of the BSE Building to the Vatican Bank before Ad Maiora purchased the BSE Building. *Id.*

### 3. Investigation 3: HSI's Current Investigation Against Matta

The Court understands that the HSI is also investigating Matta domestically for at least two alleged discrete violations of United States federal law: [REDACTED]

[REDACTED].<sup>5</sup> The Court terms this “Investigation 3.”

As it concerns [REDACTED], the Government represents that it is investigating Matta

[REDACTED]

[REDACTED] See Declaration of Special Agent

[REDACTED] dated March 8, 2024 (“[REDACTED] Mar. Decl.”), ECF 17 ¶ 2. The gist of this alleged criminality, as represented by the Government, is that Matta [REDACTED]

[REDACTED]

[REDACTED] to buy and invest in property in the United States, “[c]urrently [ ] still managed by Matta and his firm.” *Id.* ¶¶ 6-7.

The specific facts provided in SA [REDACTED] declaration only report that, at some unspecified point in time, [REDACTED] informed SA [REDACTED] that a portion of the more than 200 million euros that the IOR had invested in the Ad Maiora fund “[REDACTED] [REDACTED].” [REDACTED] Feb. Decl. ¶ 8. Further, the Government alleges that “[a]t least two funds controlled by Matta and OAM invest in commercial and residential real estate in the United States, known as USA Property I and USA Property II.” *Id.* The purported “investment

---

<sup>5</sup> In SA [REDACTED] February Declaration—[REDACTED] states that HSI has opened an “independent investigation into Matta and his related entities for potential violations of U.S. criminal laws, including [REDACTED] [REDACTED].” [REDACTED] Feb. Decl. ¶ 11. However, after the Court allowed the Government to file supplemental documentation with regard to the issue of reasonable suspicion, the Government proffered [REDACTED] March Declaration on March 8, 2024, stating that HSI is investigating Matta for the alleged violation of “[REDACTED].” The underlying specified unlawful activity under investigation is an offense involving bribery of a foreign public official, in violation of Title 18, United States Code, Section [REDACTED].” [REDACTED] Mar. Decl. ¶ 2. Therefore, the Court only addresses these two bases for reasonable suspicion.

fraud scheme perpetrated” by Matta is alleged to have involved the use of “foreign entities, formed in various jurisdictions, and involved the [REDACTED]” [REDACTED] Mar. Decl. ¶ 6. Crucially, SA [REDACTED] declaration is devoid of any specificity as to whether such information was received before or after Matta’s detention.

As to [REDACTED], the Government represents that it is investigating Matta [REDACTED] [REDACTED]. As to this purported criminality, those foreign public officials are alleged to be [REDACTED]. *Id.* ¶¶ 2-3. The Government’s investigation appears to mirror [REDACTED] [REDACTED] [REDACTED] “to obtain funding from the [Vatican Bank].” *Id.* ¶ 5. The Government represents that Cipriani “was found in 2018 by a Vatican court to have misappropriated Vatican government funds [REDACTED] [REDACTED].” *Id.* However, the Government does not allege nor do any other facts appear to actually connect Matta to the [REDACTED] [REDACTED]. And, again, SA [REDACTED] declaration does not state *when* HSI received this information.

SA [REDACTED] supplemental March declaration further declares that “Matta and his firm maintain the capacity to store, transact, and maintain financial records concerning these assets.” *Id.* ¶ 6. SA [REDACTED] asserts that [REDACTED] [REDACTED] [REDACTED] [REDACTED] *Id.* There is no evidence provided as to when this “information” was relayed to HSI nor

were specific facts proffered implicating Matta of criminal activity—to the extent that the Government is asserting Matta violated United States federal law.

### **C. Matta’s Arrival to New York on October 7, 2023**

On October 5, 2023, SA [REDACTED] determined that Matta would be taking Iberia flight 6251 from Madrid to New York, set to arrive to JFK airport on October 7, 2023. Feb. Decl. R. ¶ 12. On October 6, 2023, SA [REDACTED] submitted a “request” to HSI at JFK to search Matta at the U.S. border and detain his electronic devices. [REDACTED] Feb. Decl. ¶ 12.

On October 7, 2023, Matta traveled from Madrid, Spain, to New York City, disembarking at JFK airport. Matta Decl. ¶¶ 4-5. Upon Matta’s production of his passport to a Customs and Border Protection (“CBP”) agent (“CBP Agent 1”), Matta was brought to a separate room to speak to another agent (“CBP Agent 2”). *Id.* ¶ 5. Matta asserts that he was questioned by the CBP Agent 2 for about 40 minutes. *Id.* ¶¶ 6-7. CBP Agent 2 asked Matta an array of questions about his city of departure, his itinerary, and the purpose of his travel. *Id.* Matta stated that he was traveling for business.<sup>6</sup> *Id.* Matta inquired as to the purpose of the questioning, to which “CBP Agent 2 responded repeatedly that he did not know the purpose and that he was following instructions.” *Id.*

#### **1. Production of Electronic Devices on October 7, 2023**

After the conclusion of Matta’s questioning, CBP Agent 2 asked Matta to produce all of the electronic devices in his possession and place them on the table. Matta Decl. ¶ 8. Matta then produced one cell phone, a Samsung Galaxy (“Cellphone”), and one Microsoft laptop computer (“Laptop”) (together the “Subject Devices”). *Id.* After placing the Subject Devices on the table,

---

<sup>6</sup> On October 7, 2023, upon arrival in the United States, Matta informed U.S. CBP officers that the purpose of his travel was to meet with clients and investors. Redacted Declaration of SA [REDACTED] dated March 8, 2024, (“Mar. Decl. R.”), ECF 19-2 ¶ 8.

Matta asserts that CBP Agent 2 began to physically inspect and photograph both devices. *Id.* CBP Agent 2 asked Matta for the brand and model of the Cellphone and if he had any other devices in his possession. Matta obliged and confirmed that he did not have any other devices. Nonetheless, CBP Agent 2 searched Matta's bag for more devices and did not find any other device. *Id.*

## **2. Search of Cellphone on October 7, 2023**

Thereafter, CBP Agent 2 asked Matta to provide the password for the Cellphone. Matta Decl. ¶ 9. Matta declined and asked to speak with his lawyer before doing so. *Id.* Matta asserts he had already declined to give his passcode when "CBP Agent 2 then showed [Matta] a pre-printed piece of a paper that he claimed reflected CBP Agents rights to inspect electronic devices." *Id.* Matta explains in his declaration that he declined to provide his passcode because he was concerned about "revealing sensitive business and personal information, including communications and documents that are protected by attorney-client privilege and work product doctrine." *Id.* CBP Agent 2 continued to ask for Matta to unlock his Cellphone to review its contents. *Id.*

At some point, a third CBP Agent ("CBP Agent 3"), who appears to already have been present in the detention room, was summoned by CBP Agent 2 to approach the desk where Matta was seated. CBP Agent 3 also asked Matta to unlock his Cellphone so that CBP Agent 3 could help CBP Agent 2 "identify and record the International Mobile Equipment Identity (IMEI) number" of Matta's Cellphone. *Id.* ¶ 10. Matta then used his fingerprint to unlock his Cellphone and handed it over to the CBP agents. *Id.* The CBP agents then "operated" the phone and recorded the IMEI number. *Id.* Throughout his time in CBP detention Matta queried the CBP Agents multiple times as why he was being questioned and searched. *Id.* CBP Agent 2 replied that he did not know. *Id.*



### **3. Seizure of Cellphone and Laptop and Encounter with Homeland Security Agent on October 7, 2023**

At some point after the IMEI number was identified and the Cellphone had been “operated,” an HSI agent, Thomas Wilbert (“Agent Wilbert”), entered the detention room and advised Matta that the Subject Devices would be detained. Matta Decl. ¶¶ 10-11. Agent Wilbert then asked Matta for an address to which he could later deliver the Subject Devices. *Id.* Matta asked Agent Wilbert why his devices were being detained. *Id.* Agent Wilbert stated that he could not provide Matta with any information as to the reason for their detention. *Id.* Agent Wilbert gave Matta a receipt for the Subject Devices and informed Matta that he was free to leave. *Id.* According to Matta, his encounter with CBP and HSI at the border lasted approximately 80-90 minutes. *Id.* ¶ 12.

#### **D. Correspondence with HSI after Seizure of Matta’s Devices**

On the morning of October 13, 2023, Matta’s personal attorney, Richard Albert (“Attorney Albert”), emailed Agent Wilbert advising him that he represented Matta and requesting to speak with the agent by phone. Richard Albert Declaration (“Albert Decl.”), ECF 1-2 ¶ 5a; *see also* Exhibit A, Email correspondence with HSI Agent (“Oct. 13 emails”), ECF 1-3. Agent Wilbert replied later that same day, informing Attorney Albert that the Cellphone would be returned on October 16, 2023, but the Laptop would continue to be detained by the Government. Albert Decl. ¶ 5b. “Soon after,” Attorney Albert replied to Agent Wilbert reiterating his request for a phone call with him or a government attorney involved in the matter of the detained Subject Devices but received no response. *Id.* ¶ 5c.

#### **E. Return of the Cellphone and Laptop - Continued Correspondence With HSI**

On October 17, 2023, the Cellphone was delivered by mail to Attorney Albert at his office. Albert Decl. ¶ 6. Upon receipt, Attorney Albert sent a letter via email to Agent Wilbert asking him

to advise whether digital copies had been made of the Subject Devices, whether data from the Subject Devices had been searched by the Government, and the legal basis for the seizure and any searches. *Id.* ¶ 7. Attorney Albert also notified Agent Wilbert that the electronic devices contained “sensitive business information, including extensive communications and other information protected by the attorney-client privilege and work-product doctrine,” and that Matta and Optimum were fully asserting those privileges and all other privileges related to the electronic devices. *Id.*; *see also* Exhibit B, Letter Correspondence with HSI Agent Wilbert (“Oct. 17 Letter”), ECF 1-4.

On October 19, 2023, after having received no response from Agent Wilbert, Attorney Albert called the First Assistant United States Attorney for the Eastern District of New York to inquire about the Subject Devices—however, Attorney Albert was unsuccessful in obtaining any further information as to who was involved in the search and seizure of Matta’s electronic devices. Albert Decl. ¶ 8.

On October 23, 2023, with the Laptop still in the Government’s possession and with no response from Agent Wilbert, Attorney Albert emailed a letter to the Executive Associate Director of HSI and Special Agent in Charge of the New York field office of HSI. *Id.* ¶ 9. However, no response was received. *Id.* ¶ 9b; *see* Exhibit C, Letter to HSI Director and Special Agent, ECF 1-5. On October 30, 2023, Attorney Albert received an email from Agent Wilbert asking if he would like the Laptop to be sent to his office. Albert Decl. ¶ 10. In its Opposition, the Government reported to the Court that the Laptop was returned to Petitioner’s attorney on October 31, 2023. *See* Government’s Response or Answer to Complaint (“Gov. Opp.”), ECF 8 at 2.

#### **F. Search and Seizure of Matta’s Electronic Devices**

During oral argument the Government stated that after the Subject Devices were detained at JFK, they remained locked and unable to be accessed. *See* Oral Argument Transcript (“Tr.”) at

6. The Subject Devices were then sent to the New York CBP technology team within a couple of days after their detention to determine whether the technology team could “unlock” the Subject Devices. *Id.* The technology team was able to “unlock” Matta’s Cellphone. *Id.*

### 1. Matta’s Cellphone

HSI created a forensic image of Matta’s Cellphone. [REDACTED] Feb. Decl. ¶ 16. On November 3, 2023, SA [REDACTED] and two other agents from HSI Rome met with [REDACTED] and requested assistance in examining the contents of Matta’s Cellphone. *Id.* ¶ 15. The federal agents “informed [REDACTED] that [the Subject Devices] may contain contents that are protected by the attorney-client privilege and instructed them to make all efforts necessary to separate any content that may be protected by the attorney-client privilege, including through the use of a privilege review team, consistent with the ICE Directive.” *Id.* Based on the facts provided to the Court by the Government, it appears that [REDACTED] searched the contents of the Petitioner’s Cellphone because “[REDACTED] [REDACTED] confirmed to [SA [REDACTED] its implementation of a separate ‘filter team’ that is reviewing the content of the phone for any privilege content. Non-privileged content is being subjected to a second review to determine the existence of evidence or contraband related to [an] alleged financial fraud scheme,” discussed further below. *Id.* ¶ 16; Feb. Decl. R. ¶ 16.

On March 7, 2024, the Government concluded its search of Matta’s Cellphone and identified in its contents alleged “[e]vidence of cross-border criminal activity.” March 8 Letter from Government (“Mar. Gov. Ltr.”), ECF 17 at 1. Three forensic copies of the Cellphone were created.<sup>7</sup> The Government has represented that “a copy of ten WhatsApp message threads and

---

<sup>7</sup> The Government’s letter indicated that “[t]he original [forensic image of Petitioner’s Cellphone] [REDACTED]

[REDACTED] Mar. Gov. Ltr. at fn 2.

their attachments have been extracted in order to be used in the ongoing criminal investigation of Petitioner, including by the U.S. Attorney's Office in the Southern District of Florida, which is evaluating evidence.” *Id.* at 1-2. However, the Government further represents that the forensic “images” of the contents of Matta’s Cellphone “will not be re-accessed without a court order.” *Id.*

## **2. Matta’s Laptop**

The Government reported in a subsequent filing that “Matta’s laptop has not been examined because it is encrypted and, despite repeated attempts, HSI has not been able to access the contents of the laptop.” January 29, 2024, Letter Filed *Ex Parte* and Under Seal (“Jan. 29 Ltr. R.”), ECF 15 at 3. SA [REDACTED] also reported in his February declaration that he found it unlikely that law enforcement would be able to access the laptop with currently available forensic tools. Feb. Decl. R. ¶ 17. “On February 14, 2024, HSI deleted the copy of the forensic encrypted image of the laptop and retains no data or information from the laptop (other than the serial number of the laptop).” *Id.* This was further confirmed by the Government’s March 8, 2024, letter stating, “[a]s set forth in the February 16, 2024, Declaration of Special Agent [REDACTED] the forensic encrypted image of Petitioner’s Microsoft Surface Book laptop was not subjected to a border search because HSI was unable to access it. The forensic image was deleted on February 14, 2024, and HSI retained no data or information from the laptop other than the laptop’s serial number.” March 8 Letter from Government Redacted (“Mar. Gov. Ltr. R.”), ECF 19 at fn 1.

## **PROCEDURAL HISTORY**

On October 30, 2023, Matta filed the instant Motion. *See* Motion for Return of Property. On November 9, 2023, the Government filed a motion for an extension of time to file an answer, ECF 4, which the Court granted on November 13, 2023, directing the Government to file its response by November 16, 2023. *See* Docket Entry dated 11/13/23. On November 14, 2023, the

Government requested a further extension of time, ECF 6, which the Petitioner opposed, ECF 7. The Court granted the Government's second extension request, directing it to file its answer on or by December 15, 2023. *See* Docket Entry dated 11/16/23.

On December 15, 2023, the Government filed its response in opposition to Petitioner's motion. *See* Gov. Opp. On December 22, 2023, the Petitioner filed a reply to the Government's opposition. Petitioner's Reply ("Matta Reply"), ECF 9. On January 8, 2024, the Government filed a sur-reply. Government's Reply in Opposition ("Gov. Sur-Reply"), ECF 10.

On January 12, 2024, the Court set oral argument on the Motion for February 6, 2024. Docket Entry dated 01/12/24. Thereafter, Petitioner filed for an adjournment, ECF 11, and the Court reset the argument for January 31, 2024. On January 31, 2024, the Court held oral argument on the Motion. *See* Minute Entry dated 01/31/24. Neither side presented witnesses nor introduced further evidence. As discussed further below, the parties' arguments before the Court centered on the proper standard of review of such forensic border searches and the support for the search in the instant matter.<sup>8</sup> *See generally* Transcript.

On March 8, 2024, the Government filed a motion to file an additional memorandum of law and a supplementary declaration from SA [REDACTED]<sup>9</sup> On March 18, 2024, the Government

---

<sup>8</sup> On January 29, 2024, the Government sought leave to electronically file documents *ex parte* and in camera/under seal. On February 2, 2024, the Court granted in part and denied in part the Government's request for leave to file in camera/under seal, directing the Government to submit a redacted version of the documents for its consideration. *See* Docket Entry dated 02/02/24. On February 16, 2024, the Government refiled their request for seal with proposed redactions for the Court's review. ECF 13. On February 20, 2024, the Petitioner filed a response in opposition to the Government's seal request. Petitioner's response to 02/16/24 Seal Request ("Pet. Opp. to 2/16/24 Seal req."), ECF 14. On March 1, 2024, the Court granted the Government's seal request and directed the Government to file the redacted submissions from 02/16/24. Additionally, on March 1, 2024, the Court declared that the Government may "submit *ex parte* and under seal any further factual evidence by March 8, 2024, along with a memorandum of no more than 2 pages...The submissions must also be accompanied by a proposed and 'narrowly tailored' redacted version of each" related to the specific issue of reasonable suspicion. Docket Entry dated 03/01/24. On March 4, 2024, the Government filed a redaction of the January 29, 2024, letter filed *ex parte* and under seal, *see* Jan. 29 Ltr. R., and the redaction of SA [REDACTED] Declaration in Support of Government's Response to Petitioner's Application for Return of Property, *See* Feb. Decl. R.

<sup>9</sup> Thereafter on March 12, 2024, Petitioner filed a request to unseal the March 4, 2024, submissions, and requested either partial or full access to the March 8, 2024, submissions. Petitioner's Request to Unseal, ECF 18. On March

filed the redacted version of the March 8, 2024, Sealed filings. *See* Government Second Memorandum of Law (“Gov. Memo R.”), ECF 19-1; *see* Mar. Decl. R.; Mar. Gov. Ltr. R. On April 1, 2024, the Petitioner filed a Reply to the Government’s second memorandum of law. Petitioner’s Second Reply (“Pet. Sur-Reply”), ECF 20.<sup>10</sup>

### LEGAL STANDARD

Rule 41(g) of the Federal Rules of Criminal Procedure allows “[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property [to] move for the property’s return ... If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.” Fed. R. Crim. P. 41(g).

District courts in this Circuit have applied a three-part test that a moving party must pass to prevail on a Rule 41(g) motion: “(1) [the party] is entitled to lawful possession of the seized property; (2) the property is not contraband; and (3) either the seizure was illegal or the government’s need for the property as evidence has ended.” *United States v. Morgan*, 443 F. Supp. 3d 405, 407 (W.D.N.Y. 2020)(collecting cases). “The court must receive evidence on any factual issue necessary to decide the motion.” *United States v. Alvarez-Estevez*, 671 F. App’x 834, 835 (2d Cir. 2016). An order requiring the return of property under Rule 41(g) “is an equitable remedy that is available only when there is no adequate remedy at law and the equities favor the exercise of jurisdiction.” *De Almeida v. United States*, 459 F.3d 377, 382 (2d Cir. 2006).

---

14, 2024, the Court granted the Government’s motion for leave to seal directing them to file the redacted submission onto the docket. Docket Entry dated 3/14/24.

<sup>10</sup> For clarity, the sealed filings that were filed *ex parte* by the Government are the following: Government’s First Motion for Sealed Documents January 29, 2024, Letter (“Jan. Gov. Ltr.”), ECF 12; Government’s Second Motion for Sealed Documents including: [REDACTED] Feb. Decl., ECF 13-1 and refile of Jan. Gov. Ltr, ECF 13-2; Government’s Third Motion for Sealed documents including: Mar. Gov. Ltr., Government’s Second Memorandum of Law (“Gov. Memo”), and [REDACTED] Mar. Decl., ECF 17.

## DISCUSSION

The resolution of the instant Motion turns solely on the third prong, that is whether the Government’s search and seizure of the contents of Matta’s Cellphone was illegal, *i.e.*, in violation of the Fourth Amendment.<sup>11</sup> The Court addresses the relevant legal principles below.

### A. Fourth Amendment

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. CONST. AMEND. IV. The “basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” *Carpenter v. United States*, 585 U.S. 296, 303 (2018). The Fourth Amendment “expressly imposes two requirements. First, all searches and seizures must be reasonable. Second, a warrant may not be issued unless probable cause is properly established, and the scope of the authorized search is set out with particularity.” *Kentucky v. King*, 563 U.S. 452, 459 (2011). “In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.” *Riley v. California*, 573 U.S. 373, 382 (2014). As the text of the Fourth Amendment makes clear, “the ultimate touchstone of the Fourth Amendment is ‘reasonableness.’” *Id.* at 381-82.

“Nevertheless, because the ultimate touchstone of the Fourth Amendment is ‘reasonableness,’ the warrant requirement is subject to certain exceptions.” *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) (citing *Flippo v. West Virginia*, 528 U.S. 11, 13 (1999) (*per curiam*)). In defining whether an exception to the warrant requirement should be recognized, courts

---

<sup>11</sup> The Government concedes that “Matta’s laptop has not been examined because it is encrypted.” Feb. Decl. R ¶ 17. “Despite repeated attempts, HSI has not been able to access the contents of the laptop” and on “February 14, 2024, HSI deleted the copy of the forensic encrypted image of the laptop and retains no data or information from the laptop (other than the serial number of the laptop).” *Id.* In light of these admissions, and for the purposes of Petitioner’s pending Motion, the Court only addresses the search and seizure of Matta’s Cellphone as it was the only device that was actually de-encrypted and forensically copied and is currently in the Government’s possession.

focus on the search’s reasonableness and consider, on the one hand, “the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *United States v. Miller*, 430 F.3d 93, 97 (2d Cir. 2005); *United States v. Fox*, 23-CR-227 (NGG), 2024 WL 3520767, at \*6 (E.D.N.Y. July 24, 2024).

### **1. Warrant Exception for Border Searches**

One judicially recognized exception to the warrant requirement arises out of the so-called border search doctrine. As the Supreme Court has explained, a traveler seeking entry into the United States at the international border has a diminished expectation of privacy. *See United States v. Montoya de Hernandez*, 473 U.S. 531, 539-40 (1985) (citing *Florida v. Royer*, 460 U.S. 491, 515 (1983) (Blackmun, J., dissenting)). This diminished expectation of privacy arises out of the surveillance and security measures needed to monitor air travel. *Id.* Searches made pursuant to the so-called border-search exception are justified by “the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country” which makes such searches “reasonable simply by virtue of the fact that they occur at the border. . . .” *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

Searches at the international border, where “the [g]overnment’s interest in preventing the entry of unwanted persons and effects is at its zenith,” *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), have long been exempt from the warrant requirement. *Id.* at 152-53. “Although this exception is broad, it is not unfettered.” *United States v. Kamaldoss*, 19-CR-543 (ARR), 2022 WL 1200776, at \*9 (E.D.N.Y. Apr. 22, 2022). While the Supreme Court has not spoken to the precise circumstances under which some level of suspicion is required for a border search, it has suggested that “‘in the case of highly intrusive searches’ where salient ‘dignity and privacy



interests’ are at stake, ‘a requirement of . . . suspicion’ might be supported.” *See id.* (quoting *Flores-Montano*, 541 U.S. at 152).

## 2. Routine Versus Non-Routine Border Searches

Within the confines of the border-search doctrine, courts have distinguished between “routine” and “non-routine” searches. Routine searches include: “searches of outer clothing, luggage, a purse, wallet, pockets, or shoes. . . .” *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006). Such routine searches do not require a warrant or even reasonable suspicion to be reasonable under the Fourth Amendment. *See Montoya*, 473 U.S. at 538.

Non-routine border searches, however, require weighing the “offensiveness of the intrusion” against “the level of warranted suspicion[.]” *Irving*, 452 F.3d at 123; *see also Flores-Montano*, 541 U.S. at 152. Non-routine searches that are highly intrusive generally require at least reasonable suspicion, for example—invasive searches such as strip searches or alimentary canal searches rise to the level of intrusion that requires heightened analysis. *See Irving*, 452 F.3d at 123. Searches of certain personal items in which an individual has a heightened privacy interest may also require reasonable suspicion. *See United States v. Levy*, 803 F.3d 120, 123 (2d Cir. 2015) (considering whether copying the contents of a traveler’s notebook required reasonable suspicion but finding it unnecessary to resolve this issue); *but see Flores-Montano*, 541 U.S. at 154-55 (rejecting a privacy interest in a motorist’s gas tank and approving suspicion-less border searches asserting the government had the authority to “remove, disassemble, and reassemble a vehicle’s fuel tank.”). The Second Circuit and several other circuits have since recognized that more invasive searches, such as strip searches, are non-routine, thus requiring reasonable suspicion.<sup>12</sup>

---

<sup>12</sup> *See also United States v. Kolsuz*, 890 F.3d 133, 144-47 (4th Cir. 2018); *United States v. Gonzalez-Rincon*, 36 F.3d 859, 864 (9th Cir. 1994); *United States v. Yakubu*, 936 F.2d 936, 939 (7th Cir. 1991); *United States v. Oyekan*, 786 F.2d 832, 837-39 (8th Cir. 1986).

*Irving*, 452 F.3d at 123. Whether a search is so intrusive that it crosses into the territory of non-routine hinges upon how “deeply [the search] intrudes into a person’s privacy.” *Kolsuz*, 890 F.3d at 144; *accord Kamaldoss*, 2022 WL 1200776, at \*31-32 (citing to *Irving*, 452 F.3d at 123 (noting that non-routine searches are those that “substantially infringe on a traveler’s privacy rights”))).

In this case, Petitioner takes the position that the off-site forensic searches of the contents of the Subject Devices were non-routine—asserting that at least reasonable suspicion<sup>13</sup> was required for CBP to conduct the search. *See* Pet. Memo at 5-6; Matta Reply at 3-6. In taking this position, Petitioner relies on the Supreme Court’s decision in *Riley*, 573 U.S. 373, 395 (2014), which discussed and opined on the heightened privacy interest in personal electronic devices in arguing that at least reasonable suspicion should apply. *See* Pet. Memo at 5-6. Petitioner urges the Court to consider two recent decisions from other courts of appeal that found forensic searches of cellphones and other personal devices at border crossings constituted as non-routine border searches. *See United States v. Cano*, 934 F.3d 1002, 1014-16 (9th Cir. 2019); *United States v. Aigbekaen*, 943 F.3d 713, 720-21 (4th Cir. 2019).

The Government’s opposition does not address Petitioner’s privacy arguments. Rather, the Government takes the position that the searches it conducted on Petitioner’s Devices were lawful. Gov. Opp. at 3-4. While the Government acknowledges that the Second Circuit has not yet defined the contours of routine and non-routine border searches as they relate to electronic devices, the Government argues that even if reasonable suspicion was required it had such reasonable suspicion. *Id.*

---

<sup>13</sup> Petitioner also argues that Judge Rakoff’s decision in *United States v. Smith*, 2023 WL 3358357, at \*8 (S.D.N.Y. May 11, 2023), in which that Court extended *Riley*’s warrant requirement for cellphone data searches incident to arrests to the border context, should also hold here. The Government stridently rejects probable cause is required. Gov. Memo Redacted, at 2. The Government acknowledges that, at most, reasonable suspicion was required—“a relatively low standard and border officials are afforded deference due to their training and experience.” *Id.* at 3 (quoting *Abidor v. Napolitano*, 990 F. Supp. 2d 260, 282 (E.D.N.Y. 2013)). However, because the Court concludes the Government lacked even the requisite reasonable suspicion to search the Cellphone, it need not address this argument.

Neither the Second Circuit nor the Supreme Court have yet to opine as to whether forensic searches of electronic devices detained by agents at the border are definitively routine or non-routine. *See Fox*, 2024 WL 3520767, at \*7. Thus, the Court finds it prudent to review what privacy interests are at stake when the Government searches a cellphone and how, if at all, those interests might change in the context of a stop at the border.

### **3. Privacy Interests Implicated in Cellphone Searches Requires Reasonable Suspicion**

The Court agrees with Petitioner that such inquiries should start with *Riley*. In *Riley*, the Supreme Court held that officers must generally secure a warrant prior to searching an arrestee's cellphone. 573 U.S. at 386. In so doing, the Court acknowledged that in certain searches incident to arrest the Government has valid interests at stake, such as officer safety and preventing the destruction of evidence. *Id.* at 387-92. However, these safety and retention interests are not significantly implicated in the context of officers reviewing digital data on a cellphone. *See id.* Moreover, the Court concluded the warrant requirement must be maintained in such instances because the capabilities of modern cellphones raise heightened privacy interests: "Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so." *Id.* at 394; *see also United States v. Alisigwe*, 22-CR-425 (VEC), 2023 WL 8275923, at \*4 (S.D.N.Y. Nov. 30, 2023). In so doing, the Supreme Court addressed the "interrelated privacy consequences" in the storage capacity of phones in identifying that:

[b]efore cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos... First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible.

Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records.

*Riley*, 573 U.S. at 375.

The Court reaffirmed the principle that simply because new “technology now allows an individual to carry [a vast quantity of personal] information in his hand” that “does not make the information any less worthy of the protection for which the Founders fought.” *Id.* at 403.

Since *Riley*, the public’s continued reliance on technology reaffirms the importance of the foundational protections surrounding privacy interest. These protections remain ever prominent in the context of the advancements and capabilities of modern-day electronic devices. The Second Circuit has more recently held that “the search and seizure of personal electronic devices like a modern cellphone or tablet computer implicates different privacy and possessory concerns than the search and seizure of a person’s ordinary personal effects.” *United States v. Smith*, 967 F.3d 198, 208 (2d Cir. 2020). Importantly here, the Circuit has also held that a comprehensive forensic search of a computer, whether a desktop or a laptop, involves a significant invasion of privacy. *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013).

Given the foregoing, the Court agrees with Petitioner and finds that a non-routine border search of an international traveler’s personal electronic device resulting in offsite forensic imaging and copying, like what occurred here with the Subject Devices, requires the Government to have at least reasonable suspicion given the heightened privacy interests in the contents of such personal electronic devices.<sup>14</sup> *See Cotterman*, 709 F.3d at 966; *Abidor v. Napolitano*, 990 F. Supp. 2d 260,

---

<sup>14</sup> The Court acknowledges that a recent decision in this district held that non-routine border searches or personal electronic devices such as cellphones and tablets requires a warrant. *See United States v. Sultanov*, 22-CR-149 (NRM), 2024 WL 3520443 (E.D.N.Y. July 24, 2024). The Court is aware of this case and notes that the parties in this current action have not yet had an opportunity to brief the issue in light of this decision. In any case, *Sultanov* does not change the outcome here as the Court concludes that the Government fails to even meet the lower burden of reasonable suspicion.

280-83 (E.D.N.Y. 2013); *United States v. Smith*, 673 F. Supp. 3d 381, 396 (S.D.N.Y. 2023) (discussing at length the heightened privacy interests in cellphones and reduced government interests due to the nature of digital data and finding that officers violated the defendant’s Fourth Amendment rights where the search of a cellphone was not for digital contraband nor evidence of digital contraband); *Alisigwe*, 2023 WL 8275923, at \*5 (“[C]ellphone searches cannot be conducted without reasonable suspicion of criminal activity because they are not routine border searches.”); *United States v. Gavino*, 22-CR-136 (RPK), 2024 WL 85072, at \*6 (E.D.N.Y. Jan. 7, 2024) (“[R]easonable suspicion of criminal activity suffices to justify a cell-phone border search.”); *Aigbekaen*, 943 F.3d at 720 (intrusive, non-routine searches of an electronic device require some level of individualized suspicion).

With the standard of suspicion settled, the Court turns to the heart of this motion: whether on October 7, 2023, any federal law enforcement officer had articulable facts amounting to reasonable suspicion that Matta had committed or was committing any prosecutable crimes and whether either of the Subject Devices had nexus to those crimes.

## **B. Reasonable Suspicion**

The reasonable suspicion analysis simply requires the Court, after considering all the facts of a particular case, to determine “whether the border official ha[d] a reasonable basis on which to conduct the search.” *United States v. Asbury*, 586 F.2d 973, 976 (2d Cir. 1978). Reasonable suspicion demands “specific and articulable facts which, taken together with rational inferences from those facts . . . provide . . . officers with a particularized and objective basis for suspecting wrongdoing.” *United States v. Bailey*, 743 F.3d 322, 332 (2d Cir. 2014).

The Second Circuit has provided lower courts with several factors they may consider in making the reasonable suspicion determination including unusual conduct of the defendant,

discovery of incriminating matter during routine searches,<sup>15</sup> computerized information showing a propensity to commit relevant crimes,<sup>16</sup> or a suspicious itinerary. *See Irving*, 452 F.3d at 124. Further, “[r]easonable suspicion may be based upon information from a confidential informant so long as the tip bears sufficient ‘indicia of reliability.’” *United States v. Elmore*, 482 F.3d 172, 179 (2d Cir. 2007) (quoting *Adams v. Williams*, 407 U.S. 143, 147 (1972)). “As in the probable cause context, courts must assess whether an informant’s tip establishes reasonable suspicion under the totality of the circumstances approach set forth in *Illinois v. Gates*, 462 U.S. 213 (1983), though obviously a lesser showing is required.” *Id.* (citation omitted).

Although in *Gates* the Supreme Court abandoned the rigid two-pronged test of *Aguilar v. Texas*, 378 U.S. 1083 (1964), and *Spinelli v. United States*, 393 U.S. 410 (1969), the informant’s ‘basis of knowledge’ and ‘veracity’ (i.e., how he knows and why we should believe him) remain highly relevant to a determination of either probable cause or reasonable suspicion.

*Id.* (quoting *Alavama v. White*, 496 U.S. 325, 328-29 (1990)).

### **1. The Government Fails to Establish that Reasonable Suspicion of Criminality Existed Prior to October 7, 2023**

While the Government argues that the detention and search of Petitioner’s devices was lawful and that the Government has a continued need for the data, Gov. Opp. at 2, the Government asserts in the alternative that reasonable suspicion was nonetheless present.<sup>17</sup> Gov. Opp. at 2-4.

---

<sup>15</sup> *See e.g., United States v. Asbury*, 586 F.2d 973, 977 (2d Cir. 1978) (finding reasonable suspicion for a strip search at the border where prior to traveler’s “arrival, border officials had received word from a source previously found to be reliable that a couple answering appellants’ descriptions was suspected of carrying contraband. Upon arrival, appellant Bruce was one of the first to leave the plane but one of the last to present himself for customs inspection. He changed inspection lanes while awaiting inspection. He wore loose-fitting clothing. He had made a side trip to Thailand, a well-known narcotics source. He had shipped several suitcases back to the United States prior to his return. His demeanor, including eye contact and speech, was unusual”).

<sup>16</sup> *See, e.g., Abidor v. Napolitano*, 990 F. Supp. 2d 260, 267, 282–83 (E.D.N.Y. 2013) (finding reasonable suspicion for further inspection of a traveler’s electronic devices where, among other indicia of suspicion, the traveler had two visas in a foreign passport, an inspection of the travelers’ device border agents observed images of the rallies of designated terrorist groups (Hamas) on the laptop computer, and the fact that the traveler had recently traveled to Lebanon).

<sup>17</sup> As noted above, the Court gave the Government several opportunities to establish reasonable suspicion through supplemental briefing. *See Infra* fn 4.

The Government asserts that the relevant standard here in determining the “reasonableness” of the search pursuant to the Fourth Amendment, is satisfied by “(1) tips or leads from informants or other reliable sources and (2) computerized information entered by law enforcement personnel showing pertinent criminal propensities.” Gov. Memo Redacted at 3 (citing *Asbury*, 586 F.2d at 976-77). The Government contends that reasonable suspicion is established by the information it received from [REDACTED] and/or through HSI’s own investigation regarding Plaintiff’s alleged bribery of Vatican Bank officials and defrauding of the Vatican Bank, including in relation to the BSE transaction. *See generally* [REDACTED] Declarations.

“[W]hether a Custom’s official’s reasonable suspicion arises entirely from her own investigation or is prompted by another federal agency is irrelevant to the validity of a border search.” *Irving*, 803 F.3d at 123. However, this proposition assumes that there is actual evidence in the record of the reasonable suspicion held by at least one officer involved in either requesting or conducting the search. *United States v. Bongiovanni*, 19-CR-227 (JLS) (MJR), 2022 WL 17481884, at \*13 (W.D.N.Y. Aug. 5, 2022), *report and recommendation adopted*, 19-CR-227(JLS)(MJR), 2022 WL 17139489 (W.D.N.Y. Nov. 22, 2022). Here, the Court finds that there is no evidence in the record of reasonable suspicion at the time of the border search.

The two declarations provided by HSI SA [REDACTED] the sole proffer made by the Government to establish reasonable suspicion—consists almost entirely of background facts relating to: (1) the Vatican Bank’s history with Matta, including the decade’s worth of contentious litigation—which Matta already confirmed in his moving papers, *see generally* [REDACTED] Feb. Decl.; *See generally* Suriano Decl.; (2) [REDACTED], [REDACTED] Feb. Decl. ¶ 4; (3) [REDACTED], [REDACTED] Mar. Decl. ¶ 5; (4) an

assertion that [REDACTED]

[REDACTED], which was affirmed on appeal, *id.*; and (5) general information about Matta’s business involvement in Europe and in the United States, Mar. Decl. R. ¶ 4; *see generally* [REDACTED] Feb. Decl.

It is black letter law that “[i]n evaluating whether an officer had reasonable suspicion, [a court] look[s] only to the facts that the officer knew at the time of the stop. Any events that occur after a stop is effectuated cannot contribute to the analysis of whether there was reasonable suspicion to warrant the stop in the first instance.” *United States v. Veloz-Lopez*, 595 F. App’x 81, 82 (2d Cir. 2015) (citing *United States v. Freeman*, 735 F.3d 92, 96 (2d Cir.2013)) (summary order); *accord United States v. Barnes*, 22-CR-109 (ER), 2022 WL 12399322, at \*3 (S.D.N.Y. Oct. 21, 2022) (“Like probable cause, reasonable suspicion is determined based on the totality of the circumstances known to the officers *at the time of the stop*.” (cleaned up)). That is the Court’s only inquiry is as to whether “the facts available to the officer at the moment of the seizure or the search ‘warrant a man of reasonable caution in the belief’ that the action taken was appropriate.” *United States v. Arenas*, 37 F. Supp. 2d 322, 326 (S.D.N.Y. 1999) (internal citation omitted).

Even assuming *arguendo* that the veracity and trustworthiness of tips from [REDACTED] amounted to reasonable suspicion, the Government’s submissions fail to establish that such sufficient information was known to law enforcement or relayed to the detaining officer *prior* to Matta’s detention on October 7, 2023. The Court has instead been left to parse through the Government’s ambiguously worded declaration to identify the essential factual pictures of exactly “who knew what when.” *Cf. Aguilar v. Immigr. & Customs Enf’t Div. of U.S. Dep’t of Homeland Sec.*, 255 F.R.D. 350, 361 (SD.N.Y. 2008) (“With probable cause generally out of the



picture, ‘who knew what when’ is, at best, only marginally relevant.”); *see also United States v. Int’l Bhd. of Teamsters*, 708 F. Supp. 1388, 1396 (S.D.N.Y. 1989) (explaining that the “underlying the difficulties in these complaints is the factual basis for alleging that the fraudulent parties had knowledge of the falsity of such statements at the time they were made. The question of timing and specificity becomes paramount in a securities fraud case because liability is premised on who knew what when.”).

As explained above, the HSI received at some unknown time information that led to the Government initiating an “investigation” into potential [REDACTED] and [REDACTED]. However, there are no articulatable facts provided by the Government, who carries the burden here, for the Court to conclude that any such information was within the knowledge of HSI or the Government prior to October 7, 2023. Further, even if the Government had such knowledge prior to the seizure and search of the Subject Devices, the Government has failed to carry its burden of demonstrating it possessed “specific and articulable facts which, taken together with rational inferences from those facts . . . provide . . . officers with a particularized and objective basis for suspecting wrongdoing.” *Bailey*, 743 F.3d at 332.

The Court notes that while the Government alleges, through information gained from [REDACTED] that Matta is allegedly involved with an “investment fraud scheme,” [REDACTED] Mar. Decl. ¶ 6, the only cited violations of any U.S. federal law enforceable by the Government are for [REDACTED] and [REDACTED]. *Id.* ¶ 2. Notwithstanding that such “investment fraud” is not a standalone crime under federal law—and that nothing akin to securities fraud has been alleged here—the Government failed to provide evidence of reasonable suspicion of any prior or ongoing criminal conduct.

Moreover, the Government does not further elucidate any theory of investment fraud in its letter brief. The fact that Matta employs “foreign entities, formed in various jurisdictions, and involved the re-assignment of shares to transfer ownership” is not on its own illegal conduct. [REDACTED] Mar. Decl. ¶ 6. Nor is the mere fact that Matta has “current business ties to the U.S., including significant investments in U.S.-based real estate” provide any articulatable suspicion of any kind of cognizable federal fraud. Gov. Memo at 3. Moreover, the veracity of the statement that Matta was actually involved in any “investment fraud scheme” arising from conduct alleged to have occurred over a decade ago in the sale of the BSE building is not supported by any actual evidence—such as a foreign fraud judgment. In fact, Matta’s own submissions allege that the Vatican Bank has in fact “repeated losses in court proceedings in various jurisdictions in Europe” regarding the BSE sale. *See* Suriano Decl. ¶¶ 2, 5, and 6. The Government does not provide a rebuttal to this, despite repeated opportunities to respond.

As to the suspicion of Matta’s involvement in bribing of a public official, the Government again fails to actually proffer any specific or articulable facts that would actually support criminal activity. Instead, the Government seeks for this Court to draw a tenuous inference that because [REDACTED]

[REDACTED] that Matta must have had something to do with it because of Matta’s and Optimum’s work through Ad Maiora. [REDACTED] Mar. Decl. ¶ 5 (emphasis added). Yet again, no specific facts are proffered that actually tie Matta, now or in October 2023, to Cipriani’s “misappropriation of funds” much less to infer that he bribed Cipriani or any other public official. The Court is left with conclusory connect-the-dot allusions and mere hunches which cannot suffice. Indeed, the Fourth Amendment requires “some minimal level of objective justification” prior to law enforcement searches such as this. *INS v. Delgado*, 466 U.S.

210, 216-17 (1984). A mere “inchoate and unparticularized suspicion or ‘hunch’” will not suffice. *United States v. Sokolow*, 490 U.S. 1, 7 (1989) (quoting *Terry v. Ohio*, 392 U.S. 1, 27 (1968)).

Lastly, as to [REDACTED], the Government states that “[a]t least two funds controlled by Matta and OAM invest in commercial and residential real estate in the United States, known as USA Property I and USA Property II.” [REDACTED] Feb. Decl. ¶ 8. Property ownership in and of itself is not illegal. Additionally, the fact that [REDACTED] informed SA [REDACTED] at some unspecified time, “[REDACTED] [REDACTED],” *see id.*, also provides no evidence of criminality for the reasons just stated. No actual or specific evidence of fraud involving Ad Maiora in the United States has been disclosed to the Court. The only facts established, insofar as the Court is aware, are that the Vatican Bank has pursued Matta in foreign jurisdictions since 2013 in connection with its dissatisfaction of Matta’s informal disclosure during the BSE Building sale and has for the past 11 years been without any legal success. While the Court appreciates the international cooperation of law enforcement, unsubstantiated allegations of involvement in criminal activity should not impede upon Fourth Amendment rights even for foreign travelers entering this country.<sup>18</sup>

Moreover, Petitioner correctly points out that the cases relied on by the Government are distinguishable because in each of those cases the officer was presented with additional specific and articulable facts in the record suggesting the traveler was involved in criminal activity.<sup>19</sup> *See*,

---

<sup>18</sup> *See United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985) (finding that the respondent, a non-U.S. citizen entering into the U.S., “[h]aving presented herself at the border for admission and having subjected herself to the criminal enforcement powers of the Federal Government, 19 U.S.C. § 482, [ ] was entitled to be free from unreasonable search and seizure.”).

<sup>19</sup> Here there are no articulable facts to suggest ongoing criminal activity. *Cf. Ramirez*, 2019 WL 3502913 (reasonable suspicion where TECS record entry indicated defendant was linked to purchase of child pornography and initial consent search revealed suspected images of child pornography); *Cotterman*, 709 F.3d at 957-58 (reasonable suspicion based on TECS alert as well as agents’ discovery of defendant’s prior child-related conviction, the fact that he was returning from a country associated with sex tourism, and his possession of multiple electronic devices); *Kamaldoss*,

*e.g.*, *United States v. Gavino*, 22-CR-136 (RPK), 2024 WL 85072, at \*6 (E.D.N.Y. Jan. 7, 2024) (reasonable suspicion found where traveler was “traveling with \$37,000 in cash on his person, which was seized but never retrieved, was behavior consistent with narcotics trafficking.”); *Alisigwe*, 2023 WL 8275923, at \*6 (finding reasonable suspicion existed where the London-based informant informed the HSI that Alisigwe was using multiple identities and possessed a fraudulent passport); *United States v. Levy*, 803 F.3d 120, 123 (2d Cir. 2015)(reasonable suspicion found where a “review of the allegations in the initial underlying indictment against Levy (filed within days of the search) and the allegations in the subsequent, superseding indictment confirm that the search was justified by the CBP officer’s reasonable suspicion of Levy’s ongoing criminal participation in securities fraud schemes. In fact, the level of suspicion was so high that Levy himself was aware of his status as a target of an ongoing federal investigation even prior to arriving at the airport, and his lawyer previously had contacted federal prosecutors about the investigation”).

Of course, if there existed reasonable suspicion that Matta was involved in criminal activities such as complex money laundering or wire fraud, there would be a strong basis for law enforcement to believe that evidence of such activity might be found on Matta’s Cellphone and Laptop. But, as it stands, the Government has failed to proffer any concrete individualized findings of any such criminal engagement and thus any search is void.<sup>20</sup>

---

2022 WL 1200776 (reasonable suspicion of defendant’s involvement in transnational conspiracy where investigation revealed controlled buys, information from a confidential informant, and seized packages mailed by defendant containing contraband).

<sup>20</sup> *See, e.g.*, *United States v. Watson*, 23-CR-82(EK), 2023 WL 7300618, at \*4 (E.D.N.Y. Nov. 6, 2023) (“Even before consideration of the agent’s expertise and experience, common sense dictates that evidence of a complex, long-duration financial fraud are likely to be found on the electronic devices of the alleged leader of that activity. Moreover, courts have repeatedly relied on agents’ training and experience with electronic devices and the criminal conduct at issue generally—taken together with information known about a specific defendant’s conduct—to find the existence of probable cause for the seizure of electronic devices.”).

Given the foregoing, the Court finds that the seizure and subsequent forensic search and duplication of Matta's Cellphone on October 7, 2023, was a non-routine border search that required reasonable suspicion of criminal activity. Further, the Court finds that the Government has not met its burden of proof of showing that HSI Agents had reasonable suspicion of any criminal activity at the time they conducted the search. Therefore, the Court concludes that the forensic search of the Cellphone, which started at the border and continued off-site, was unreasonable and in violation of Matta's Fourth Amendment rights.

**C. Remedy Available to Petitioner Under Fed. R. Crim. P. 41(g)**

Initially, Petitioner brought this Rule 41(g) action seeking three forms of relief:

- 1) Return to Mr. Matta his Microsoft laptop computer identified by serial number 002729104057 (the "laptop") and all copies of data obtained from the Laptop;
- 2) Return to Mr. Matta all copies of data derived from Mr. Matta's Samsung Galaxy Cellphone identified by International Mobile Equipment Identification number 353055152108298511 (the "cellphone"); and
- 3) Identify all searches or reviews conducted of Mr. Matta's laptop or cellphone.

Proposed Order to Show Cause, ECF 1.

Given that both parties concede that Matta's physical Laptop and Cellphone have been returned to the Petitioner, the Court turns to the relief regarding the forensic copies of contents and any remaining data of the Subject Devices—in particular the content and data of Matta's Cellphone.

Rule 41(g) motions are available as equitable relief "only when there is no adequate remedy at law and the equities favor the exercise of jurisdiction." *De Almeida*, 459 F.3d 377 at 382. In light of the Government's continued possession of the forensic copies of the content and data of

the Petitioner’s Cellphone, the Court grants Petitioner’s request for return of property by ordering the destruction of all records related to the Subject Devices.<sup>21</sup> Destruction of copies/records is an equitable form of relief that is recognized pursuant to Fed. R. Crim. P. 41(g). The Advisory Committee notes that Rule 41(g) contemplates not only the return but also the destruction of “copies of records.” *See* Fed. R. Crim. P. 41 (advisory committee’s note (1989 amendments) (“In some circumstances . . . equitable considerations might justify an order requiring the government to return or destroy all copies of records that it has seized.)). *See, e.g., Carpenter v. Koskinen*, 3:13-CV-563 SRU, 2015 WL 3510300, at \*8 (D. Conn. June 4, 2015) (ordering that the Government “destroy any and all copies, electronic or otherwise” of the subject property at issue seized during a search” pursuant to Rule 41(g)).

Petitioner argues that the Government should be prohibited from further disseminating forensic copies of the Subject Devices.<sup>22</sup> The Court agrees. As Rule 41(g) is an equitable form of relief, the Court must consider whether the “equities favor” the requested relief. *De Almeida*, 459 F.3d at 382. Here, the equities favor Petitioner. As discussed above, the Government has already supplied both domestic and international law enforcement agencies with the data collected and forensically copied from Matta’s Subject Devices—data obtained from an unconstitutional search that occurred on United States soil. While the Government did not have the benefit of the Court’s present ruling—to continue to allow the Government to disseminate and disclose the fruits of its unconstitutional search, Matta’s personal and purportedly privileged forensic data, would be

---

<sup>21</sup> Again, noting that the Government has represented to the Court that on “February 14, 2024, HSI deleted the copy of the forensic encrypted image of the laptop and retains no data or information from the laptop (other than the serial number of the laptop).” Feb. Decl. R. ¶ 17. However, to the extent that any remaining data or information—printed or electronic—arising out of the unconstitutional search/forensic copying of the Laptop remains in the Government’s possession, the Government is instructed to destroy such contents.

<sup>22</sup> With regard to the data obtained from Petitioner’s Subject Devices, Petitioner asserted at oral argument that it would be “problematic . . . if the Government provided any of this material to Vatican authorities so they can hand it to the litigant that [Matta] has been fighting successfully with for six years.” Tr. at 36:20-23.

inequitable and improper. The onus falls on both domestic authorities and foreign governments to assert the proper legal process to obtain access to the data contents of the Petitioner's Subject Devices. The Court concludes its within its equitable power to forbid the Government from sharing the contents and data of Petitioner's Subject Devices. *Cf. Adeleke v. United States*, 355 F.3d 144, 149 (2d Cir. 2004) ("When a court possessing equitable powers has jurisdiction over a complaint that seeks equitable relief, it has authority to award whatever damages are incident to the complaint.") (awarding equitable damages as relief in Rule 41(g) motion where property had been destroyed by the Government); *see also Franklin v. Gwinnett Cnty. Pub. Sch.*, 503 U.S. 60, 69 (1992) (acknowledging "the long line of cases in which the [Supreme] Court has held that if a right of action exists to enforce a federal right and Congress is silent on the question of remedies, a federal court may order any appropriate relief.").

However, the Court rejects Petitioner's argument that the Government must provide a list of searches it conducted on the Cellphone. By its own text, Rule 41(g) only allows for "the property's return" or, as explained above the deletion of copies in certain circumstances. It does not contemplate in any way that Rule 41(g) may be utilized by an "aggrieved person" to instruct the Government to perform other actions on property or in connection with that property, such as delivering a list of searches. As previously noted, "[j]urisdiction under Rule 41(g) is to be exercised with great restraint and caution since it rests upon the court's supervisory power over the actions of federal law enforcement officials." *De Almeida*, 459 F.3d 377 at 382. Petitioner has provided no authority nor made any argument that the equities at play here to require the Court to use its supervisory powers over the federal law enforcement in such a way. The Court rejects Petitioner's request as it does not fall within the sphere of recognized equitable relief under Rule 41(g).

## CONCLUSION

The Court finds that the Government's search and seizure of Matta's Cellphone was unconstitutional. Thus, Petitioner's Motion for Return of Property is **GRANTED** insofar as the Government must delete all copies of any data or contents taken from Matta's Subject Devices but **DENIED** as to relief sought regarding the compulsion by the Government of a list of searches.

The Court finds the following equitable relief for Petitioner:

- 1) The Government shall destroy any and all copies, electronic or otherwise any data or contents taken from Matta's Subject Devices;
- 2) The Government is forbidden from disseminating any data collected and or information from Matta's Subject Devices to any outside agencies foreign or domestic; and
- 3) The Government has 14 days from the date of this order to satisfy the equitable relief and file a sworn affidavit confirming such deletion.

**SO ORDERED.**

Dated: September 11, 2024  
Brooklyn, New York

/S/  
ORELIA E. MERCHANT  
United States District Judge